The U.S. Federal PKI and the Federal Bridge Certification Authority

Peter Alterman, Ph.D.

Senior Advisor to the Chair, Federal PKI Steering Committee

and

Acting Director, Federal Bridge Certification Authority

Introduction - Overview

The Goals of the U.S. Federal PKI

- A cross-governmental, ubiquitous, interoperable Public Key Infrastructure.
- The development and use of applications which employ that PKI in support of Agency business processes.

Why A U.S. Federal PKI?

- Statutory mandates for e-government and implementing electronic signature technology
- Demands for improved services at lower cost
- International Competition
- International Collaboration

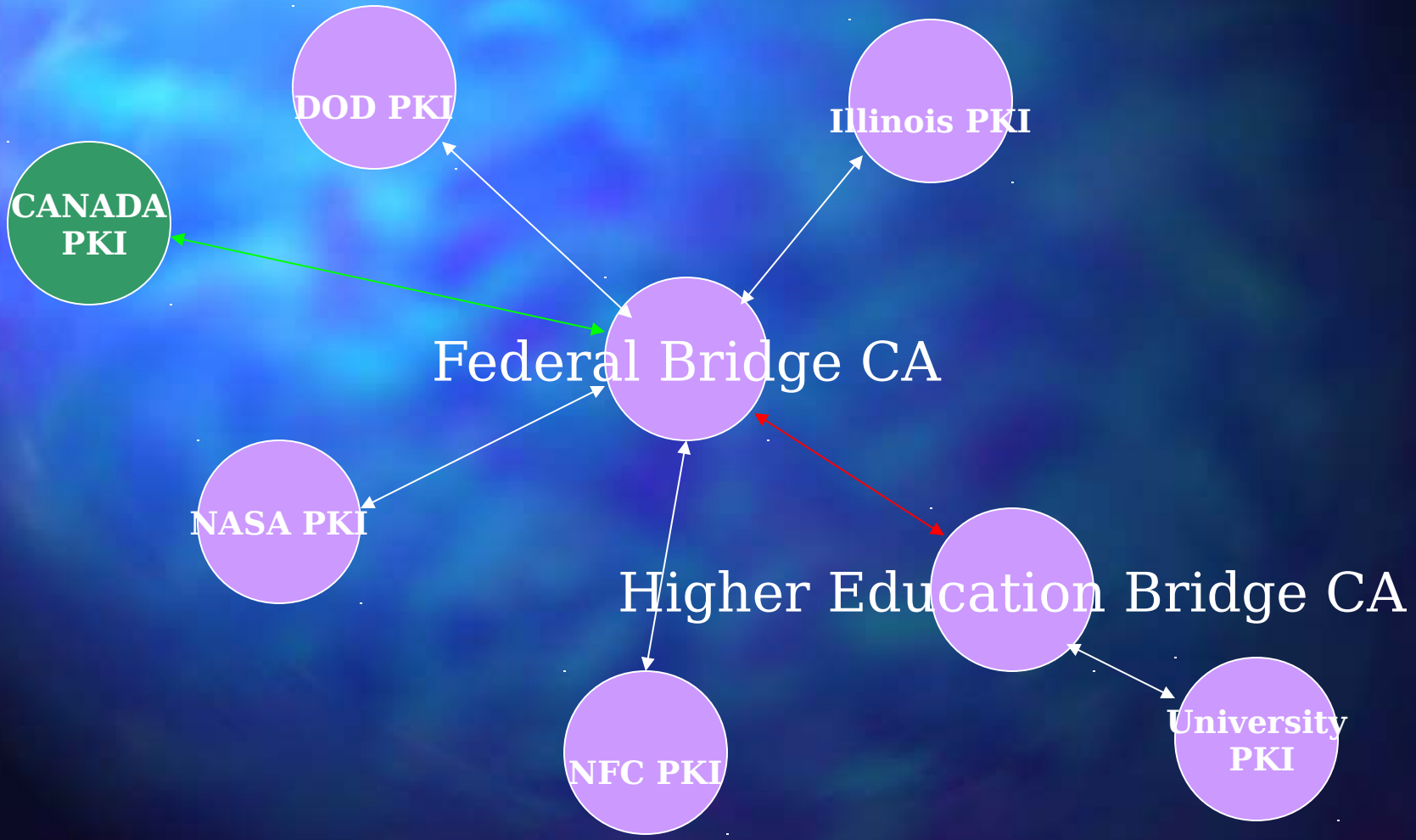
Why NOT a U.S. Federal PKI?

- Concerns of Privacy Advocates
- Agency internal politics
- Vendor battles for market space
- Cost

The Approach to a U.S. Federal PKI

- Agencies implement their own PKIs
- Create a Federal Bridge CA using COTS products to bind Agency PKIs together
- Establish a Federal PKI Policy Authority to oversee operation of the Federal Bridge CA
- Ensure directory compatibility
- Use ACES for transactions with the public

A Snapshot of the U.S. Federal PKI



The U.S. Federal Bridge Certification Authority (FBCA)

FBCA Overview

- Designed to create trust paths among individual Agency PKIs
- Employs a distributed - NOT a hierarchical - model
- Commercial CA products participate within the membrane of the Bridge
- Develops cross-certificates within the membrane to bridge the gap among dissimilar products

FBCA Goals

- Leverage emerging Agency PKIs to create a unified Federal PKI
- Limit workload on Agency CA staff
- Support Agency use of:
  - Any FIPS-approved cryptographic algorithm
  - A broad range of commercial CA products
- Propagate policy information to certificate users in different Agencies

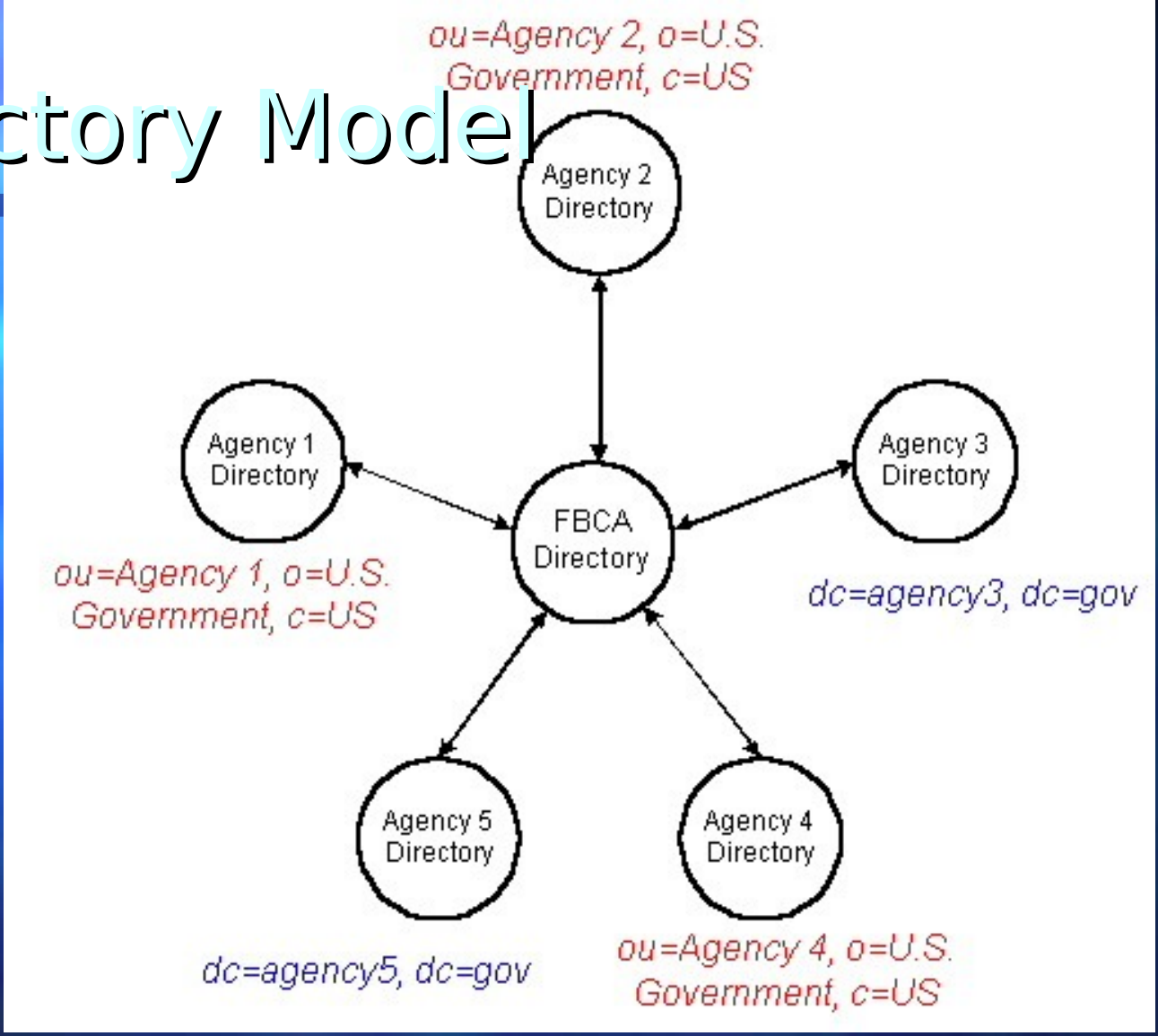
FBCA Architecture

- Multiple commercial CAs within a “membrane” that cross-certify and interoperate
- CAs offline
- No network connectivity (CA sneaker net to directory)
- FBCA directory online 24 X 7 X 365

FBCA Directory Architecture

- Chained X.500 directories
- Dual-rooted FBCA directory is “hub”
  - dc=gov
  - o=U.S. Government, c=US
- LDAP supported for non-X.500 directories

Directory Model



FBCA Operation

- Issues Certificates **to Participating CAs only**
- FPKI Steering Committee oversees FBCA development and operations
  - Documentation
  - Enhancements
  - Client-side software
- Operates in accordance with Policy Authority and FPKISC direction

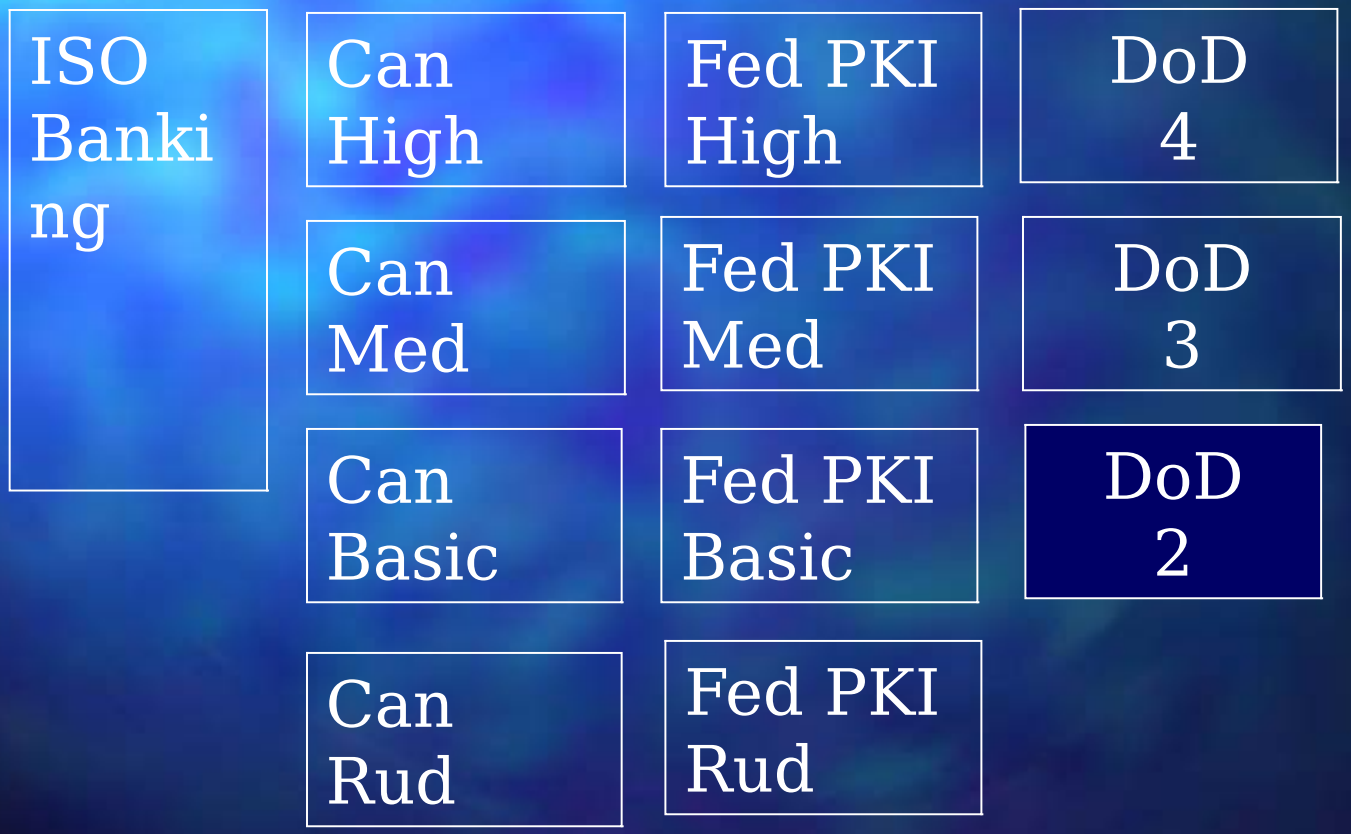
FPKI Policy Authority

- Determines participants and levels of cross-certification
  - Participants become voting members
- Administers Certificate Policy
- Enforces compliance by member organizations
- General Services Administration serves as Operational Authority

Policy Mapping

- Candidate Certificate Policies evaluated against the FBCA CP for adequacy and levels of assurance:
  - Identity binding
  - CA security
- Performed by the Federal Policy Management Authority Certificate Policy Working Group with contractor support
- Requirements publicly available on NIST website

Policy Equivalence Example



Policy Mapping Example

Federal High = DoD CLASS 4
Federal Medium = DoD CLASS 3
Bridge CA
Federal High = Canadian High
Federal Medium = Canadian Medium
DoD CA
Canadian CA
DoD CLASS 4 = Federal High
DoD CLASS 3 = Federal Medium
Canadian High = Federal High
Canadian Medium = Federal Medium
DoD CLASS 3 Subscriber
DoD CLASS 3 Subscriber
Can. HIGH Subscriber
Can. MED Subscriber

References

- Federal PKI Steering Committee Website: http://www.cio.gov/fpkisc
- NIST PKI Website: http://csrc.nist.gov/pki
- ANSI Website: http://www.ansi.org
- IETF Website: http:/www.ietf.org

Acknowledgements

- Thanks to:
  - Judith Spencer, Chair, Federal PKI Steering Committee
  - Tim Polk, National Institute of Standards and Technology
  - Dave Fillingham, National Security Agency